PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-113587
(43)Date of publication of application : 21.04.2000

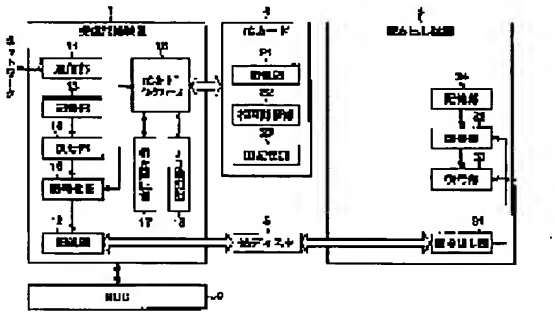
(51)Int.CI. G11B 20/10
G09C 1/00
H04L 9/14
H04L 9/32

(21)Application number : 10-282226
(22)Date of filing : 05.10.1998

(71)Applicant : SONY CORP
(72)Inventor : ISHIBASHI YOSHITO
ASANO TOMOYUKI
KITAMURA IZURU
KITAHARA ATSUSHI

(54) RECORDING DEVICE AND ITS METHOD, DECRYPTION DEVICE AND ITS METHOD, PROVISION MEDIUM AS WELL AS INFORMATION RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To enable the utilization of encrypted information in devices exclusive of a device to which the information is supplied while preventing the illicit utilization thereof by executing mutual authentication with an information memory medium, encrypting a first key with a second key and recording the encrypted information and the encrypted first key to the memory medium.
SOLUTION: An encryption section 15 reads a key for movement out of the memory section 21 of an IC card 4, again encrypts the decrypted content key with the key for movement and records the key on an optical disk 5. When the ID read out of the ID memory section 23 of the IC card 4 is decided to be not registered in an ID identification section 18 and is decided to be not mutually authenticated with the IC card 4, the ID identification section 18 or a mutual authentication section 17 executes prescribed error processing. The mutual authentication section 17 decrypts received random numbers with the previously stored common key and if the random numbers coincide with the random numbers before the encryption, the IC card 4 is authethenticated as the correct IC card.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－113587
（P2000－113587A）
(43)公開日　平成12年４月21日(2000.4.21)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｄ０４４
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ	５Ｋ０１３
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１	
9/32			６７５Ａ	

審査請求　未請求　請求項の数12　ＯＬ　（全 11 頁）

(21)出願番号　特願平10－282226

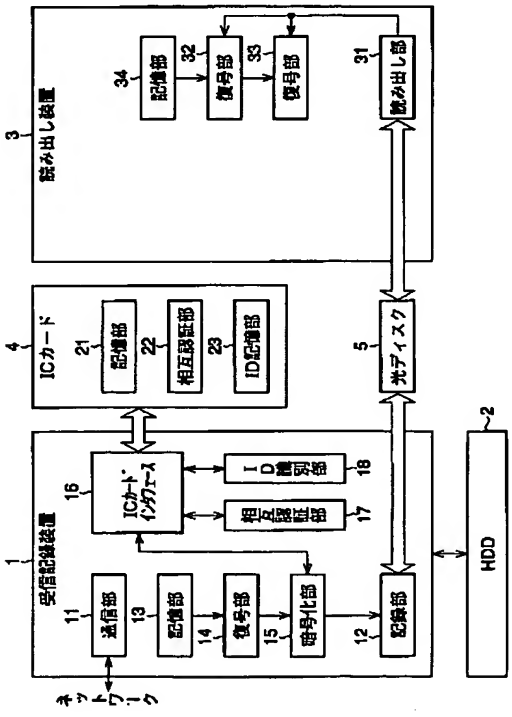
(22)出願日　平成10年10月５日(1998.10.5)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　石橋　義人
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　浅野　智之
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

最終頁に続く

(54)【発明の名称】　記録装置および方法、復号装置および方法、提供媒体、並びに情報記録媒体

(57)【要約】
【課題】　不正な利用を防止しつつ、暗号化された情報を、情報が供給された装置以外で利用できる。
【解決手段】　相互認証部１７は、ICカード４と相互認証する。暗号化部１５は、移動用鍵で、コンテンツ鍵を暗号化する。記録部１２は、暗号化されたコンテンツ、および暗号化部１５により暗号化されたコンテンツ鍵を光ディスク５に記録する。



【特許請求の範囲】

【請求項１】　暗号化された情報、および前記情報を復号する第１の鍵を受信し、装着された記録媒体に前記情報を記録するとともに、第２の鍵を記憶する情報記憶媒体が装着される、記録装置において、
前記情報記憶媒体と相互認証する相互認証手段と、
前記相互認証手段による前記相互認証に基づいて、前記情報記憶媒体から読み出された前記第２の鍵で、前記第１の鍵を暗号化する暗号化手段と、
前記暗号化された情報、および前記暗号化手段により暗号化された前記第１の鍵を前記記録媒体に記録する記録手段とを備えることを特徴とする記録装置。

【請求項２】　前記情報記憶媒体は、前記記録媒体に記録された情報を読み出しする読み出し装置を特定するデータをさらに記憶し、
前記読み出し装置を特定するデータを識別する識別手段をさらに備えることを特徴とする請求項１に記載の記録装置。

【請求項３】　暗号化された情報、および前記情報を復号する第１の鍵を受信し、装着された記録媒体に前記情報を記録するとともに、第２の鍵を記憶する情報記憶媒体が装着される、記録装置の記録方法において、
前記情報記憶媒体と相互認証する相互認証ステップと、
前記相互認証ステップでの前記相互認証に基づいて、前記情報記憶媒体から読み出された前記第２の鍵で、前記第１の鍵を暗号化する暗号化ステップと、
前記暗号化された情報、および前記暗号化ステップで暗号化された前記第１の鍵を前記記録媒体に記録する記録ステップとを含むことを特徴とする記録方法。

【請求項４】　暗号化された情報、および前記情報を復号する第１の鍵を受信し、装着された記録媒体に前記情報を記録するとともに、第２の鍵を記憶する情報記憶媒体が装着される、記録装置に、
前記情報記憶媒体と相互認証する相互認証ステップと、
前記相互認証ステップでの前記相互認証に基づいて、前記情報記憶媒体から読み出された前記第２の鍵で、前記第１の鍵を暗号化する暗号化ステップと、
前記暗号化された情報、および前記暗号化ステップで暗号化された前記第１の鍵を前記記録媒体に記録する記録ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項５】　暗号化された情報、および前記情報を復号する暗号化された鍵が記録されている記録媒体が装着され、前記情報を復号する復号装置において、
前記記録媒体から読み出しされた前記鍵を復号する第１の復号手段と、
前記第１の復号手段により復号された前記鍵で、前記暗号化された情報を復号する第２の復号手段とを備えることを特徴とする復号装置。

【請求項６】　装着された、前記鍵を復号する第２の鍵が記憶されている情報記憶媒体と相互認証する相互認証手段をさらに備え、
前記第１の復号手段は、前記相互認証手段が相互認証に基づいて得た前記第２の鍵で、前記暗号化された情報を復号する鍵を復号することを特徴とする請求項５に記載の復号装置。

【請求項７】　暗号化された情報、および前記情報を復号する暗号化された鍵が記録されている記録媒体が装着され、前記情報を復号する復号装置の復号方法において、
前記記録媒体から読み出しされた前記鍵を復号する第１の復号ステップと、
前記第１の復号ステップで復号された前記鍵で、前記暗号化された情報を復号する第２の復号ステップとを含むことを特徴とする復号方法。

【請求項８】　暗号化された情報、および前記情報を復号する暗号化された鍵が記録されている記録媒体が装着され、前記情報を復号する復号装置に、
前記記録媒体から読み出しされた前記鍵を復号する第１の復号ステップと、
前記第１の復号ステップで復号された前記鍵で、前記暗号化された情報を復号する第２の復号ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項９】　暗号化された情報を記録媒体に記録する記録装置、または暗号化されて前記記録媒体に記録された情報を復号する復号装置に装着される情報記憶媒体において、
前記記録装置または前記復号装置と相互認証する相互認証手段と、
前記暗号化された情報を復号する第１の鍵を暗号化または復号する第２の鍵を記憶する記憶手段とを備えることを特徴とする情報記憶媒体。

【請求項１０】　前記記録媒体に記録された情報を復号する復号装置を特定するデータを記憶する第２の記憶手段をさらに備えることを特徴とする請求項９に記載の情報記憶媒体。

【請求項１１】　前記第２の鍵は、前記記録装置より供給されることを特徴とする請求項９に記載の情報記憶媒体。

【請求項１２】　前記第２の鍵は、前記復号装置より供給されることを特徴とする請求項９に記載の情報記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、記録装置および方法、復号装置および方法、提供媒体、並びに情報記録媒体に関し、特に、暗号化された情報を取り扱う記録装置および方法、復号装置および方法、提供媒体、並びに情

報記録媒体に関する。

【０００２】

【従来の技術】不正な利用を防止するため音楽などの情報を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザは、その情報処理装置で情報を復号して、読み出しするシステムがある。一般に、契約にあたって、ユーザは、情報を利用する情報処理装置を特定するデータを、情報提供者に登録する。情報提供者は、その装置に限って、情報を利用できるように、情報を暗号化して提供する。

【０００３】

【発明が解決しようとする課題】このようなシステムで供給された情報は、その情報が制限なく読み出しできる権利をユーザが取得したとしても、所定の契約を交わしたユーザが所有する他の読み出し装置では、利用できない。

【０００４】本発明はこのような状況に鑑みてなされたものであり、不正な利用を防止しつつ、暗号化された情報を、情報が供給された装置以外で利用できるようにすることを目的とする。

【０００５】

【課題を解決するための手段】請求項１に記載の記録装置は、情報記憶媒体と相互認証する相互認証手段と、相互認証手段による相互認証に基づいて、情報記憶媒体から読み出された第２の鍵で、第１の鍵を暗号化する暗号化手段と、暗号化された情報、および暗号化手段により暗号化された第１の鍵を記録媒体に記録する記録手段とを備えることを特徴とする。

【０００６】請求項３に記載の記録方法は、情報記憶媒体と相互認証する相互認証ステップと、相互認証ステップでの相互認証に基づいて、情報記憶媒体から読み出された第２の鍵で、第１の鍵を暗号化する暗号化ステップと、暗号化された情報、および暗号化ステップで暗号化された第１の鍵を記録媒体に記録する記録ステップとを含むことを特徴とする。

【０００７】請求項４に記載の提供媒体は、記録装置に、情報記憶媒体と相互認証する相互認証ステップと、相互認証ステップでの相互認証に基づいて、情報記憶媒体から読み出された第２の鍵で、第１の鍵を暗号化する暗号化ステップと、暗号化された情報、および暗号化ステップで暗号化された第１の鍵を記録媒体に記録する記録ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【０００８】請求項５に記載の復号装置は、記録媒体から読み出しされた鍵を復号する第１の復号手段と、第１の復号手段により復号された鍵で、暗号化された情報を復号する第２の復号手段とを備えることを特徴とする。

【０００９】請求項７に記載の復号方法は、記録媒体から読み出しされた鍵を復号する第１の復号ステップと、第１の復号ステップで復号された鍵で、暗号化された情報を復号する第２の復号ステップとを含むことを特徴とする。

【００１０】請求項８に記載の提供媒体は、復号装置に、記録媒体から読み出しされた鍵を復号する第１の復号ステップと、第１の復号ステップで復号された鍵で、暗号化された情報を復号する第２の復号ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【００１１】請求項９に記載の情報記憶媒体は、記録装置または復号装置と相互認証する相互認証手段と、暗号化された情報を復号する第１の鍵を暗号化または復号する第２の鍵を記憶する記憶手段とを備えることを特徴とする。

【００１２】請求項１に記載の記録装置、請求項３に記載の記録方法、および請求項４に記載の提供媒体においては、情報記憶媒体と相互認証し、相互認証に基づいて、情報記憶媒体から読み出された第２の鍵で、第１の鍵を暗号化し、暗号化された情報、および暗号化された第１の鍵を記録媒体に記録する。

【００１３】請求項５に記載の復号装置、請求項７に記載の復号方法、および請求項８に記載の提供媒体においては、記録媒体から読み出しされた鍵を復号し、復号された鍵で、暗号化された情報を復号する。

【００１４】請求項９に記載の情報記憶媒体においては、相互認証手段が記録装置または復号装置と相互認証し、記憶手段が暗号化された情報を復号する第１の鍵を暗号化または復号する第２の鍵を記憶する。

【００１５】

【発明の実施の形態】以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【００１６】すなわち、請求項１に記載の記録装置は、情報記憶媒体と相互認証する相互認証手段（例えば、図１の相互認証部１７）と、相互認証手段による相互認証に基づいて、情報記憶媒体から読み出された第２の鍵で、第１の鍵を暗号化する暗号化手段（例えば、図１の暗号化部１５）と、暗号化された情報、および暗号化手段により暗号化された第１の鍵を記録媒体に記録する記録手段（例えば、図１の記録部１２）とを備えることを特徴とする。

【００１７】請求項５に記載の復号装置は、記録媒体から読み出しされた鍵を復号する第１の復号手段（例えば、図１の復号部３２）と、第１の復号手段により復号された鍵で、暗号化された情報を復号する第２の復号手段（例えば、図１の復号部３３）とを備えることを特徴とする。

【００１８】請求項９に記載の情報記憶媒体は、記録装置または復号装置と相互認証する相互認証手段（例えば、図１の相互認証部２２）と、暗号化された情報を復号する第１の鍵を暗号化または復号する第２の鍵を記憶する記憶手段（例えば、図１の記憶部２１）とを備えることを特徴とする。

【００１９】図１は、本発明の一実施の形態である記録読み出しシステムの構成を説明するブロック図である。受信記録装置１は、DES(Data Encryption Standard)などの共通鍵暗号方式で暗号化された音楽、映像、プログラム、文字等の情報（以下、コンテンツと称する）を提供するネットワークに接続されているとともに、コンテンツ鍵ＫｃｏｎによりDESなどの共通鍵暗号方式で暗号化されているコンテンツ、および保存用鍵Ｋｓで暗号化されているコンテンツ鍵ＫｃｏｎがHDD２と、所定のバスを介して、情報を送受信する。受信記録装置１は、光ディスク５が装着され、装着された光ディスク５に暗号化されたコンテンツ等の所定のデータを記録させ、また、ICカード４が装着され、ICカード４が記憶する所定のデータを読み出す。

【００２０】コンテンツを暗号化する共通鍵暗号方式であるDESは、５６ビットの共通鍵を用い、平文の６４ビットを１ブロックとして処理する暗号方式である。DESの処理は、平文を撹拌し、暗号文に変換する部分（データ撹拌部）と、データ撹拌部で使用する鍵（拡大鍵）を共通鍵から生成する部分（鍵処理部）からなる。DESのすべてのアルゴリズムは公開されているので、ここでは、データ撹拌部の基本的な処理を簡単に説明する。

【００２１】まず、平文の６４ビットは、上位３２ビットのH_0、および下位３２ビットのL_0に分割される。鍵処理部から供給された４８ビットの拡大鍵K_1、および下位３２ビットのL_0を入力とし、下位３２ビットのL_0をＦ関数で撹拌した出力が算出される。Ｆ関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の２種類の基本変換から構成されている。次に、上位３２ビットのH_0と、Ｆ関数の出力が排他的論理和され、その結果は下位３２ビットL_1とされる。下位３２ビットL_0は、上位３２ビットH_1とされる。

【００２２】上位３２ビットのH_0および下位３２ビットのL_0を基に、以上の処理を１６回繰り返し、得られた上位３２ビットのH_{16}および下位３２ビットのL_{16}が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

【００２３】通信部１１は、ネットワークに情報を送信し、ネットワークから情報を受信する。記録部１２は、光ディスク５が装着されたとき、装着された光ディスク１２に暗号化部１５またはHDD２から供給された情報を記録させる。記憶部１３は、コンテンツ鍵Ｋｃｏｎを復号する保存用鍵Ｋｓを記憶する。復号部１４は、HDD２に記録されているコンテンツ鍵Ｋｃｏｎを、記憶部１３が記憶する保存用鍵Ｋｓで復号する。暗号化部１５は、復号部１４で復号されたコンテンツ鍵Ｋｃｏｎを、ICカードインターフェース１６を介して、ICカード４から供給された移動用鍵Ｋｔで暗号化する。

【００２４】ICカードインターフェース１６は、受信記録装置１に装着されたICカード４から供給された所定のデータを、所定の形式に変更し、暗号化部１５、ID識別部１８、または相互認証部１７に出力し、また、暗号化部１５、ID識別部１８、または相互認証部１７から供給された所定のデータを、所定の形式に変更し、装着されたICカード４に出力する。相互認証部１７は、ICカードインターフェース１６を介して、DESなどの共通鍵暗号を使用して後述する手続により、ICカード４と相互認証する。ID（Identification Data）識別部１８は、ICカードインターフェース１６を介して、ICカード４から供給された、そのICカード４に固有のIDを基に、ICカード４を識別する。

【００２５】ICカード４は、読み出し装置３と１対１の組み合わせで、共に販売され、受信記録装置１に着脱自在な構造を有し、受信記録装置１に装着したとき、対応する読み出し装置３固有のIDを供給し、ICカード４を識別させ、相互認証し、移動用鍵Ｋｔを供給する。ICカード４は、記憶部２１、相互認証部２２、およびID記憶部２３を備える。記憶部２１は、ROM(Read Only Memory)、不揮発性メモリ（EEPROM(Electric Erasable Program ROM)、フラッシュメモリ、FRAM（商標）(Ferroelectric Random Access Memory)等）で構成され、移動用鍵Ｋｔが記憶されている。相互認証部２２は、ICカードインターフェース１６を介して、DESなどの共通鍵暗号を使用して後述する手続により、受信記録装置１と相互認証する。ID記憶部２３は、ROMで構成され、そのICカード４に対応する、読み出し装置３に固有のIDを記憶する。

【００２６】受信記録装置１とバスおよびネットワークで接続されていない、例えば、自動車に取り付けられ、またはユーザが携帯して使用する読み出し装置３は、読み出し部３１、復号部３２、復号部３３、および記憶部３４を備える。読み出し部３１は、受信記録装置１により、暗号化されたコンテンツおよびコンテンツ鍵Ｋｃｏｎが記録された光ディスク５が装着されたとき、光ディスク５に記録されたコンテンツおよびコンテンツ鍵Ｋｃｏｎを読み出しする。復号部３２は、読み出し部３１が光ディスク５から読み出したコンテンツ鍵Ｋｃｏｎを、記憶部３４が記憶する移動用鍵Ｋｔで復号し、復号したコンテンツ鍵Ｋｃｏｎを復号部３３に供給する。復号部３３は、読み出し部３１が光ディスク５から読み出したコンテンツを、復号部３２から供給されたコンテンツ鍵Ｋｃｏｎで復号する。記憶部３４は、ICカード４の記憶

部２１に記憶された移動用鍵Ｋｔと同一の移動用鍵Ｋｔを記憶する。

【００２７】HDD２は、バスにより受信記録装置１と接続され、コンテンツ鍵ＫｃｏｎによりDESなどの共通鍵暗号方式で暗号化されているコンテンツ、および保存用鍵Ｋｓで暗号化されているコンテンツ鍵Ｋｃｏｎを記録している。

【００２８】次に図２のフローチャートを参照して、受信記録装置１が、HDD２が記録しているコンテンツ等を光ディスク５に記録する処理を説明する。ステップＳ１１において、受信記録装置１のICカードインターフェース１６には、ICカード４が装着される。ステップＳ１２において、受信記録装置１の記録部１２には、光ディスク５が装着される。ステップＳ１３において、受信記録装置１のID識別部１８は、ICカードインターフェース１６を介して、ICカード４のID記憶部２３に記憶された読み出し装置３のIDを読み出す。ステップＳ１４において、受信記録装置１のID識別部１８は、ICカード４のID記憶部２３から読み出されたIDが、ID識別部１８に登録されているか否かを判定し、IDがID識別部１８に登録されていると判定された場合、ステップＳ１５に進み、相互認証部１７は、ICカード４の相互認証部２２と相互認証する。相互認証の処理の詳細は、図３のフローチャートを用いて後述する。

【００２９】ステップＳ１６において、相互認証部１７は、ステップＳ１５においてICカード４と相互認証できたか否かを判定し、ICカード４と相互認証できたと判定された場合、ステップＳ１７に進み、復号部１４は、HDD２から、保存用鍵Ｋｓで暗号化されたコンテンツ鍵Ｋｃｏｎを読み出す。ステップＳ１８において、復号部１４は、読み出した、暗号化されているコンテンツ鍵Ｋｃｏｎを、記憶部１３に記憶されている保存用鍵Ｋｓで復号し、復号したコンテンツ鍵Ｋｃｏｎを暗号化部１５に供給する。

【００３０】ステップＳ１９において、暗号化部１５は、ICカードインターフェース１６を介して、ICカード４の記憶部２１が記憶する移動用鍵Ｋｔを読み出す。ステップＳ２０において、暗号化部１５は、復号されたコンテンツ鍵Ｋｃｏｎを、移動用鍵Ｋｔで、再度、暗号化し、暗号化されたコンテンツ鍵Ｋｃｏｎを記録部１２に供給する。ステップＳ２１において、記録部１２は、移動用鍵Ｋｔで暗号化されたコンテンツ鍵Ｋｃｏｎを光ディスク５に記録する。ステップＳ２２において、記録部１２は、HDD２から、コンテンツ鍵Ｋｃｏｎで暗号化されたコンテンツを読み出す。ステップＳ２３において、記録部１２は、ステップＳ２２で読み出されたコンテンツを光ディスク５に記録し、処理を終了する。

【００３１】ステップＳ１４において、ICカード４のID記憶部２３から読み出されたIDが、ID識別部１８に登録されていないと判定された場合、およびステップＳ１６において、ICカード４と相互認証されなかったと判定された場合、ステップＳ２４に進み、ID識別部１８または相互認証部１７は、所定のエラーメッセージを図示せぬディスプレイに表示するなどの所定のエラー処理を実行し、処理は終了する。

【００３２】以上のように、受信記録装置１は、コンテンツ鍵Ｋｃｏｎで暗号化されたコンテンツ、および移動用鍵Ｋｔで暗号化されたコンテンツ鍵Ｋｃｏｎを光ディスク５に記録する。

【００３３】次に図３のフローチャートを参照して、図２のステップＳ１５に対応して、２つの共通鍵Ｋｃ１，Ｋｃ２で、共通鍵暗号であるDESを用いて行われる、受信記録装置１とICカード４の相互認証の処理の詳細を説明する。ステップＳ３１において、受信記録装置１の相互認証部１７は、６４ビットの乱数Ｒ１を生成する。ステップＳ３２において、受信記録装置１の相互認証部１７は、乱数Ｒ１を予め記憶している共通鍵Ｋｃ１で暗号化する。ステップＳ３３において、受信記録装置１の相互認証部１７は、暗号化された乱数Ｒ１をICカード４の相互認証部２２に送信する。

【００３４】ステップＳ３４において、ICカード４の相互認証部２２は、受信した乱数Ｒ１を予め記憶している共通鍵Ｋｃ１で復号する。ステップＳ３５において、ICカード４の相互認証部２２は、乱数Ｒ１を予め記憶している共通鍵Ｋｃ２で暗号化する。ステップＳ３６において、ICカード４の相互認証部２２は、６４ビットの乱数Ｒ２を生成する。ステップＳ３７において、ICカード４の相互認証部２２は、乱数Ｒ２を共通鍵Ｋｃ２で暗号化する。ステップＳ３８において、ICカード４の相互認証部２２は、暗号化された乱数Ｒ１および乱数Ｒ２を受信記録装置１の相互認証部１７に送信する。

【００３５】ステップＳ３９において、受信記録装置１の相互認証部１７は、受信した乱数Ｒ１および乱数Ｒ２を予め記憶している共通鍵Ｋｃ２で復号する。ステップＳ４０において、受信記録装置１の相互認証部１７は、復号した乱数Ｒ１を調べ、ステップＳ３１で生成した乱数Ｒ１（暗号化する前の乱数Ｒ１）と一致すれば、ICカード４を適正なICカードとして認証し、一致しなければ、不正なICカードであるとして、処理を終了する。ステップＳ４１において、受信記録装置１の相互認証部１７は、復号して得た乱数Ｒ２を共通鍵Ｋｃ１で暗号化する。ステップＳ４２において、受信記録装置１の相互認証部１７は、暗号化された乱数Ｒ２をICカード４の相互認証部２２に送信する。

【００３６】ステップＳ４３において、ICカード４の相互認証部２２は、受信した乱数Ｒ２を共通鍵Ｋｃ１で復号する。ステップＳ４４において、ICカード４の相互認証部２２は、復号した乱数Ｒ２が、ステップＳ３６で生成した乱数Ｒ２（暗号化する前の乱数Ｒ２）と一致すれば、受信記録装置１を適正な受信記録装置として認証

し、一致しなければ、不正な受信記録装置であるとして処理を終了する。

【００３７】図４は、読み出し装置３がコンテンツを復号する処理を説明するフローチャートである。ステップＳ５１において、読み出し装置３の読み出し部３１は、コンテンツ鍵Ｋｃｏｎで暗号化されたコンテンツ、および移動用鍵Ｋｔで暗号化されたコンテンツ鍵Ｋｃｏｎが記録された光ディスク５が装着される。ステップＳ５２において、読み出し部３１は、装着された光ディスク５から、移動用鍵Ｋｔで暗号化されたコンテンツ鍵Ｋｃｏｎを読み出し、復号部３２に供給する。ステップＳ５３において、復号部３２は、記憶部３４に記憶された移動用鍵Ｋｔを読み出す。ステップＳ５４において、復号部３２は、移動用鍵Ｋｔでコンテンツ鍵Ｋｃｏｎを復号し、復号部３３に供給する。ステップＳ５５において、読み出し部３１は、装着された光ディスク５から、コンテンツ鍵Ｋｃｏｎで暗号化されたコンテンツを読み出し、復号部３３に供給する。ステップＳ５６において、復号部３３は、コンテンツ鍵Ｋｃｏｎでコンテンツを復号し、処理は終了する。

【００３８】このように、読み出し装置３は、光ディスク５に記録されたコンテンツを復号する。

【００３９】図５は、本発明の他の実施の形態である記録読み出しシステムの構成を説明するブロック図である。図５に示す受信記録装置１は、図１に示す受信記録装置１に対して、記憶部１３、復号部１４、暗号化部１５、ICカードインターフェース１６、相互認証部１７、およびID識別部１８が省略された構成を有する。

【００４０】図５に示すICカード４は、図１に示したICカード４と同様の構成を有するが、記憶部２１は、コンテンツ鍵Ｋｃｏｎを暗号化した（復号できる）保存用鍵Ｋｓを記憶する。

【００４１】図５に示す読み出し装置３は、図１に示された読み出し装置３に対して、記憶部３４が省略され、ICカードインターフェース４１、相互認証部４２、およびID識別部４３が加えられた構成を有する。ICカードインターフェース４１、相互認証部４２、およびID識別部４３の機能は、図１に示された受信記録装置１のICカードインターフェース１６、相互認証部１７、およびID識別部１８と、それぞれ同様であるので、その説明は省略する。

【００４２】次に図６のフローチャートを参照して、図５に示す受信記録装置１が、HDD２が記録しているコンテンツ等を光ディスク５に記録する処理を説明する。ステップＳ６１において、受信記録装置１の記録部１２は、光ディスク５が装着される。ステップＳ６２において、記録部１２は、HDD２から、保存用鍵Ｋｓで暗号化されたコンテンツ鍵Ｋｃｏｎを読み出す。ステップＳ６３において、記録部１２は、暗号化されたコンテンツ鍵Ｋｃｏｎを光ディスク５に記録する。ステップＳ６４において、記録部１２は、HDD２から、コンテンツ鍵Ｋｃｏｎで暗号化されたコンテンツを読み出す。ステップＳ６５において、記録部１２は、光ディスク５に暗号化されたコンテンツを記録する。

【００４３】このように、図５に示した受信記録装置１は、光ディスク５に暗号化されたコンテンツおよび保存用鍵Ｋｓで暗号化されたコンテンツ鍵Ｋｃｏｎを記録する。

【００４４】さらに図７のフローチャートを参照して、図５に示す読み出し装置３が、コンテンツを復号する処理を説明する。ステップＳ７１において、読み出し装置３のICカードインターフェース４１には、ICカード４が装着される。ステップＳ７２において、読み出し装置３の読み出し部３１には、光ディスク５が装着される。ステップＳ７３において、読み出し装置３のID識別部４３は、ICカードインターフェース４１を介して、ICカード４のID記憶部２３に記憶された読み出し装置３のIDを読み出す。ステップＳ７４において、読み出し装置３のID識別部４３は、ICカード４のID記憶部２３から読み出されたIDが、ID識別部４３に登録されているか否かを判定し、IDがID識別部４３に登録されていると判定された場合、ステップＳ７５に進み、相互認証部４２は、ICカード４の相互認証部２２と相互認証する。相互認証の処理の詳細は、図３のフローチャートを用いて説明したものと同様であるので、その説明は省略する。

【００４５】ステップＳ７６において、相互認証部４２は、ステップＳ７５においてICカード４と相互認証できたか否かを判定し、ICカード４と相互認証できたと判定された場合、ステップＳ７７に進み、読み出し部３１は、装着された光ディスク５から、保存用鍵Ｋｓで暗号化されたコンテンツ鍵Ｋｃｏｎを読み出し、復号部３２に供給する。ステップＳ７８において、復号部３２は、ICカードインターフェース４１を介して、ICカード２の記憶部２１から、保存用鍵Ｋｓを読み出す。ステップＳ７９において、復号部３２は、コンテンツ鍵Ｋｃｏｎを保存用鍵Ｋｓで復号する。ステップＳ８０において、読み出し部３１は、装着された光ディスク５から、コンテンツ鍵Ｋｃｏｎで暗号化されたコンテンツを読み出し、復号部３３に供給する。ステップＳ８１において、復号部３３は、コンテンツ鍵Ｋｃｏｎでコンテンツを復号し、処理は終了する。

【００４６】ステップＳ７４において、読み出されたIDがID識別部４３に登録されていないと判定された場合、およびステップＳ７６において、ICカード４と相互認証できなかったと判定された場合、ステップＳ８２に進み、ID識別部４３または相互認証部４２は、所定のエラーメッセージを図示せぬディスプレイに表示するなどの所定のエラー処理を実行し、処理は終了する。

【００４７】以上のように、図５に示した読み出し装置３は、光ディスク５に記録されたコンテンツを復号す

る。

【0048】図８は、移動用鍵Ｋｔを読み出し装置３のみが有する場合の、記録読み出しシステムの構成を説明するブロック図である。図８に示す受信記録装置１は、図１に示す場合と同様であるので、その説明は省略する。ICカード４の記憶部２１は、EEPROM(Electrically Erasable Programmable Read Only Memory)、フラッシュメモリ、強誘電体メモリなどの電気的に記憶内容を書き換えできる、汎用の不揮発性メモリで構成され、ICカード４が読み出し装置３に装着されたとき、コンテンツ鍵Ｋｃｏｎを暗号化する移動用鍵Ｋｔを記憶するようになされている。図８に示す読み出し装置３は、図５に示す場合と、ほぼ同様あり、その説明は適宜省略する。図８のICカードインターフェース４１は、相互認証部４２、およびID識別部４３に対する動作は、図５に示す場合と同様であるが、記憶部３４に対しては、記憶部３４に記憶された移動用鍵ＫｔをICカード４の記憶部２１に記憶させる動作をすることが、図５に示す場合と異なる。

【0049】図９のフローチャートを参照して、図８に示す読み出し装置３が、ICカード４に移動用鍵Ｋｔを記憶させる処理を説明する。ステップＳ９１において、読み出し装置３のICカードインターフェース４１には、ICカード４が装着される。ステップＳ９２において、読み出し装置３のID識別部４３は、ICカードインターフェース４１を介して、ICカード４のID記憶部２３に記憶された読み出し装置３のIDを読み出す。ステップＳ９３において、読み出し装置３のID識別部４３は、ICカード４のID記憶部２３から読み出された読み出し装置３のIDが、ID識別部４３に登録されているか否かを判定し、読み出し装置３のIDがID識別部４３に登録されていると判定された場合、ステップＳ９４に進み、相互認証部４２は、ICカード４の相互認証部２２と相互認証する。相互認証の処理の詳細は、図３のフローチャートを用いて説明したものと同様であるので、その説明は省略する。

【0050】ステップＳ９５において、相互認証部４２は、ステップＳ９４においてICカード４と相互認証できたか否かを判定し、ICカード４と相互認証できたと判定された場合、ステップＳ９６に進み、記憶部３４は、移動用鍵ＫｔをICカード４の記憶部２１に記憶させ、処理は終了する。

【0051】ステップＳ９３において、読み出されたIDがID識別部４３に登録されていないと判定された場合、およびステップＳ９５において、ICカード４と相互認証できなかったと判定された場合、ステップＳ９７に進み、ID識別部４３または相互認証部４２は、所定のエラーメッセージを図示せぬディスプレイに表示するなどの所定のエラー処理を実行し、処理は終了する。

【0052】以上の処理により、移動用鍵Ｋｔは、ICカード４の記憶部２１に記憶される。図８に示す受信記録装置１が、光ディスク５に暗号化されたコンテンツを記録する処理は、図２のフローチャートで説明した処理と同様である。図８に示す読み出し装置が、光ディスク５に記録されたコンテンツを復号する処理は、図４のフローチャートで説明した処理と同様である。

【0053】図１０は、保存用鍵Ｋｓを受信記録装置１のみが有する場合の、記録読み出しシステムの構成を説明するブロック図である。図１０に示す読み出し装置３は、図５に示す場合と同様であるので、その説明は省略する。図１０に示すICカード４は、図８に示す場合と、同様であるので、その説明は省略する。図１０に示す受信記録装置１は、図１に示す受信記録装置１に対して、復号部１４、および暗号化部１５が省略された構成を有する。図１０に示す受信記録装置１の記憶部５１は、コンテンツ鍵Ｋｃｏｎを暗号化した（コンテンツ鍵Ｋｃｏｎを復号できる）保存用鍵Ｋｓを記憶し、保存用鍵ＫｓをICカードインターフェース１６に供給するようになされている。

【0054】図１０の記録読み出しシステムにおいては、受信記録装置１に、ICカード４が装着されたとき、図９のフローチャートと同様の処理で、受信記録装置１の記憶部５１が記憶する保存用鍵Ｋｓが、ICカード４に記憶される。図１０に示す受信記録装置１が、光ディスク５に暗号化されたコンテンツを記録する処理は、図６のフローチャートで説明した処理と同様である。図１０に示す読み出し装置３が、光ディスク５に記録されたコンテンツを復号する処理は、図７のフローチャートで説明した処理と同様である。

【0055】以上のように、コンテンツの不正な使用を防止しつつ、所定の読み出し装置で、コンテンツを利用できる。

【0056】なお、相互認証の処理として、共通鍵暗号方式であるDESで、２つの鍵を使用する処理を説明したが、DESで、１つの鍵を使用する処理、NTT（商標）が提案するFEAL、IDEA(International Data Encription Algorithm)を使用する処理、またはRAS（Rivest-Shamir-Adleman）暗号などの公開鍵暗号を使用する処理でもよい。

【0057】また、コンテンツはDESで暗号化されるとして説明したが、FEAL、またはIDEAなどの他の共通鍵暗号方式、並びにRASなど公開鍵暗号方式で暗号化してもよい。

【0058】暗号化されたコンテンツおよび暗号化されたコンテンツ鍵Ｋｃｏｎは、光ディスク５に記録するとして説明したが、フロッピディスク、MD(Mini Disk：商標)、磁気テープなどの記録媒体でもよい。

【0059】また、ICカード４のID記憶部２３から読み出されたIDが、ID識別部１８またはID識別部４３に登録されていないとき、エラー処理をして終了すると説明したが、ID識別部１８またはID識別部４３に不正なIDを記

憶しておき、それと同一のIDがICカード４のID記憶部２３から読み出されたときも、エラー処理をして終了するようにしてもよい。

【００６０】なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【００６１】また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【００６２】

【発明の効果】請求項１に記載の記録装置、請求項３に記載の記録方法、および請求項４に記載の提供媒体によれば、情報記憶媒体と相互認証し、第２の鍵で、第１の鍵を暗号化し、暗号化された情報、および暗号化された第１の鍵を記録媒体に記録するようにしたので、不正な利用を防止しつつ、暗号化された情報を、情報が供給された装置以外で利用することが可能になる。

【００６３】請求項５に記載の復号装置、請求項７に記載の復号方法、および請求項８に記載の提供媒体によれば、記録媒体から読み出しされた鍵を復号し、復号された鍵で、暗号化された情報を復号するようにしたので、不正な利用を防止しつつ、暗号化された情報を、情報が供給された装置以外で利用することが可能になる。

【００６４】請求項９に記載の情報記憶媒体によれば、記録装置または復号装置と相互認証するとともに、暗号化された情報を復号する第１の鍵を暗号化または復号する第２の鍵を記憶するようにしたので、不正な利用を防止しつつ、暗号化された情報を、情報が供給された装置以外で利用することが可能になる。

【図面の簡単な説明】

【図１】記録読み出しシステムの構成を説明するブロック図である。

【図２】受信記録装置１が、HDD２が記録しているコンテンツ等を光ディスク５に記録する処理を説明するフローチャートである。

【図３】受信記録装置１とICカード４の相互認証の処理の詳細を説明するフローチャートである。

【図４】読み出し装置３がコンテンツを復号する処理を説明するフローチャートである。

【図５】記録読み出しシステムの構成を説明するブロック図である。

【図６】図５に示す受信記録装置１が、HDD２が記録しているコンテンツ等を光ディスク５に記録する処理を説明するフローチャートである。

【図７】図５に示す読み出し装置３が、コンテンツを復号する処理を説明するフローチャートである。

【図８】記録読み出しシステムの構成を説明するブロック図である。

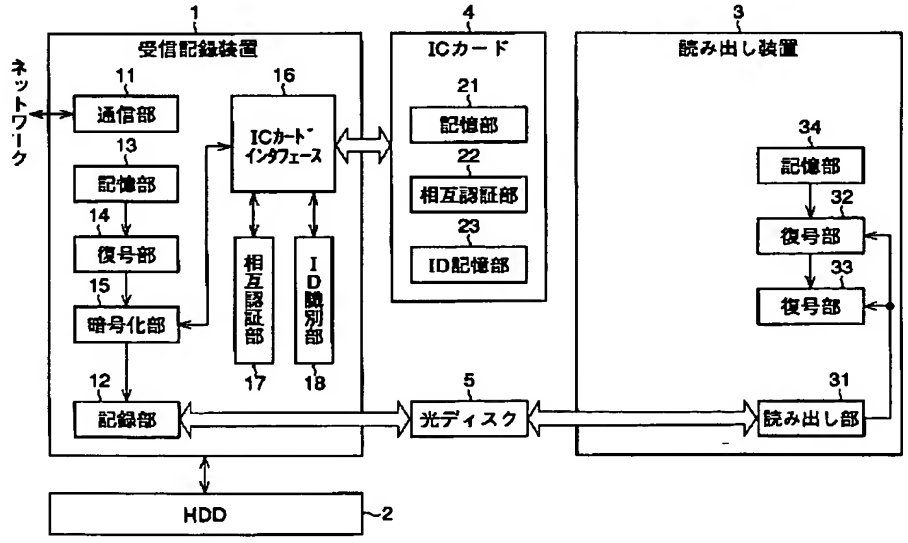
【図９】ICカード４に移動用鍵Ｋｔを記憶させる処理を説明するフローチャートである。

【図１０】記録読み出しシステムの構成を説明するブロック図である。

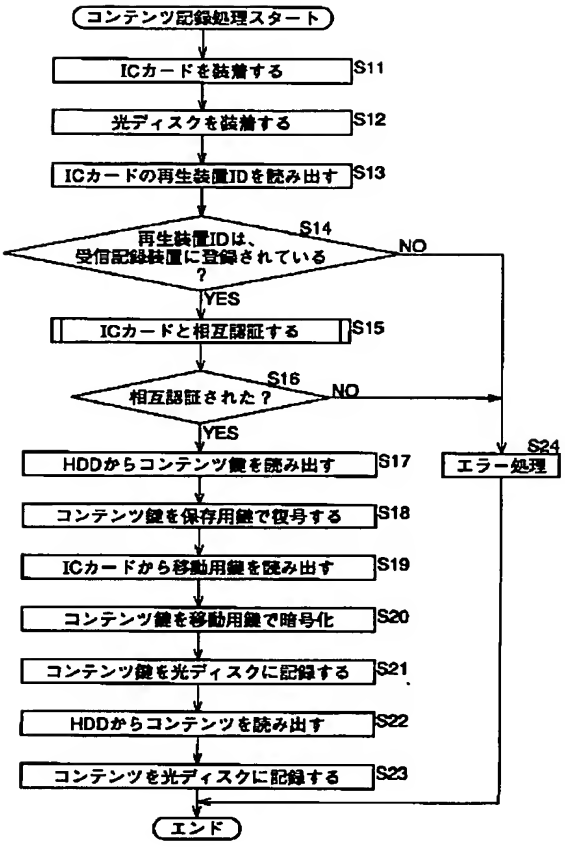
【符号の説明】

１　受信記録装置，　２　HDD，　３　読み出し装置，　４　ICカード，　５光ディスク，　１２　記録部，　１５　暗号化部，　１７　相互認証部，　２１　記憶部，　２２　相互認証部，　３２，３３　復号部

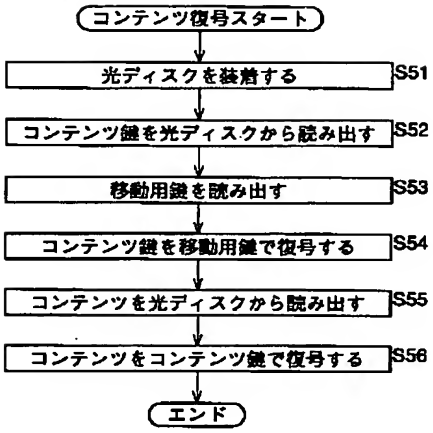
【図１】



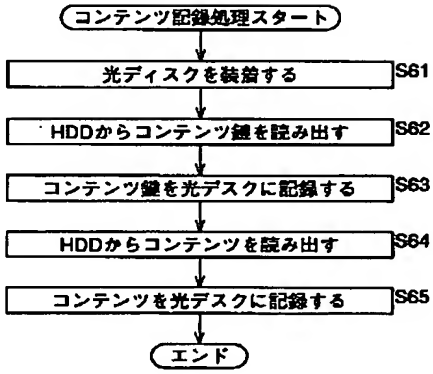
【図２】


コンテンツ記録処理スタート
ICカードを装着する
S11
光ディスクを装着する
S12
ICカードの再生装置IDを読み出す
S13
再生装置IDは、受信記録装置に登録されている？
S14
NO
YES
ICカードと相互認証する
S15
相互認証された？
S16
NO
YES
HDDからコンテンツ鍵を読み出す
S17
エラー処理
S24
コンテンツ鍵を保存用鍵で復号する
S18
ICカードから移動用鍵を読み出す
S19
コンテンツ鍵を移動用鍵で暗号化
S20
コンテンツ鍵を光ディスクに記録する
S21
HDDからコンテンツを読み出す
S22
コンテンツを光ディスクに記録する
S23
エンド

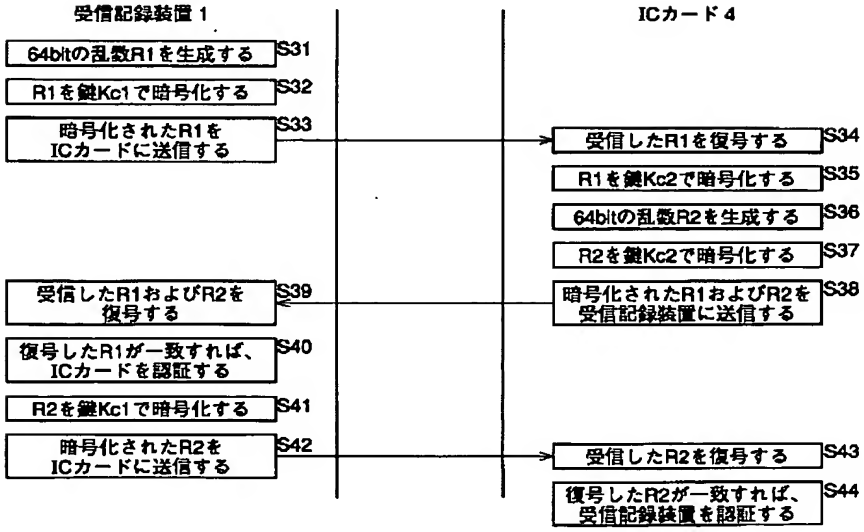
【図４】


コンテンツ復号スタート
光ディスクを装着する
S51
コンテンツ鍵を光ディスクから読み出す
S52
移動用鍵を読み出す
S53
コンテンツ鍵を移動用鍵で復号する
S54
コンテンツを光ディスクから読み出す
S55
コンテンツをコンテンツ鍵で復号する
S56
エンド

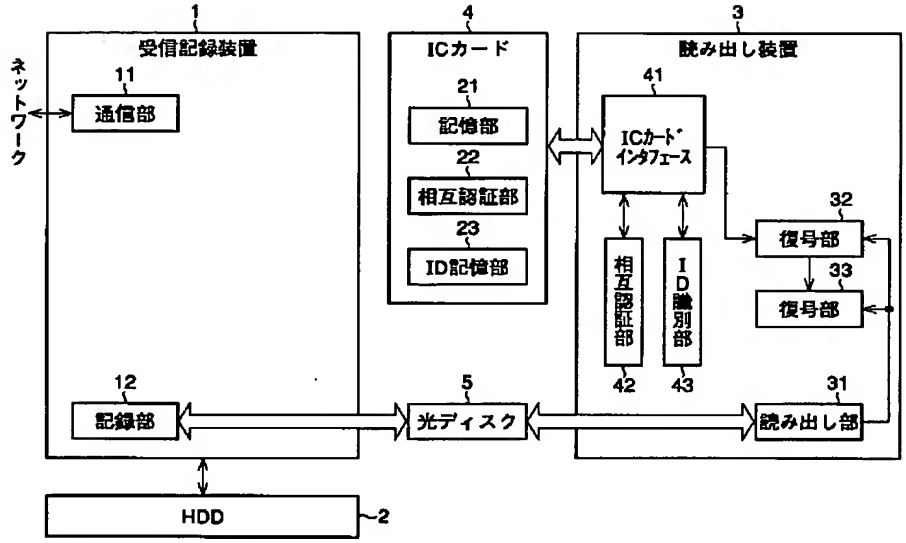
【図６】


コンテンツ記録処理スタート
光ディスクを装着する
S61
HDDからコンテンツ鍵を読み出す
S62
コンテンツ鍵を光デスクに記録する
S63
HDDからコンテンツを読み出す
S64
コンテンツを光デスクに記録する
S65
エンド

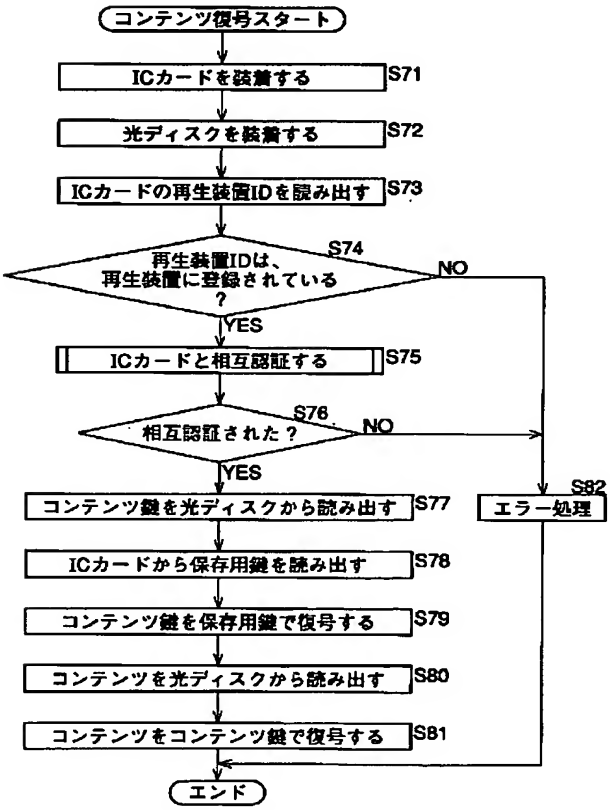
【図３】


受信記録装置１
ICカード４
64bitの乱数R1を生成する
S31
R1を鍵Kc1で暗号化する
S32
暗号化されたR1をICカードに送信する
S33
受信したR1を復号する
S34
R1を鍵Kc2で暗号化する
S35
64bitの乱数R2を生成する
S36
R2を鍵Kc2で暗号化する
S37
暗号化されたR1およびR2を受信記録装置に送信する
S38
受信したR1およびR2を復号する
S39
復号したR1が一致すれば、ICカードを認証する
S40
R2を鍵Kc1で暗号化する
S41
暗号化されたR2をICカードに送信する
S42
受信したR2を復号する
S43
復号したR2が一致すれば、受信記録装置を認証する
S44

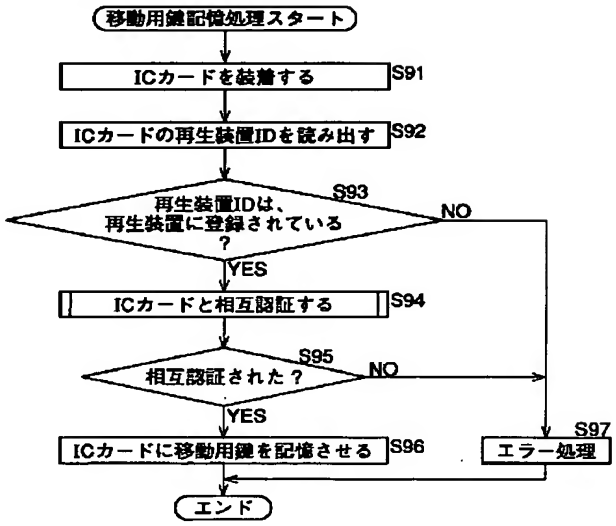
【図５】


1
受信記録装置
ネットワーク
11
通信部
12
記録部
HDD
2
4
ICカード
21
記憶部
22
相互認証部
23
ID記憶部
3
読み出し装置
41
ICカードインタフェース
相互認証部
ID識別部
42
43
32
復号部
33
復号部
5
光ディスク
31
読み出し部

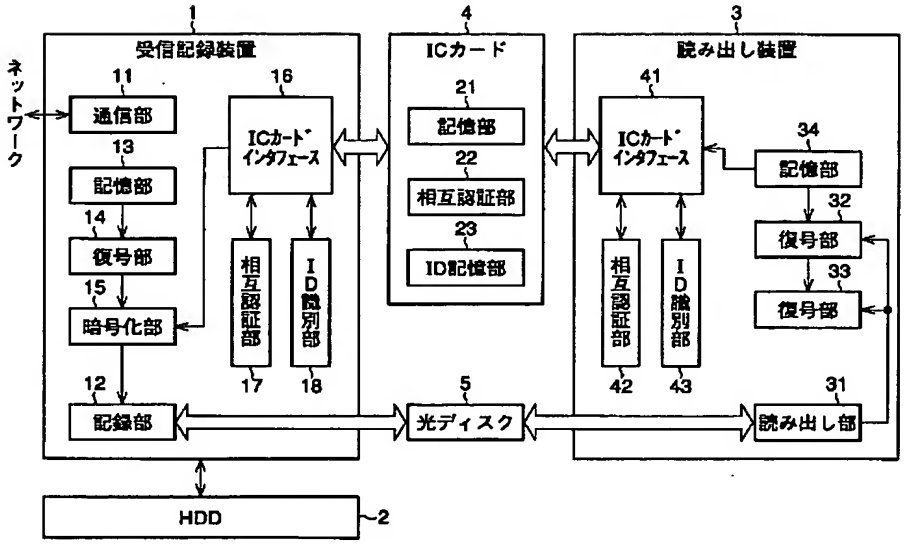
【図７】


コンテンツ復号スタート
ICカードを装着する
S71
光ディスクを装着する
S72
ICカードの再生装置IDを読み出す
S73
再生装置IDは、再生装置に登録されている？
S74
NO
YES
ICカードと相互認証する
S75
相互認証された？
S76
NO
YES
コンテンツ鍵を光ディスクから読み出す
S77
ICカードから保存用鍵を読み出す
S78
コンテンツ鍵を保存用鍵で復号する
S79
コンテンツを光ディスクから読み出す
S80
コンテンツをコンテンツ鍵で復号する
S81
エラー処理
S82
エンド

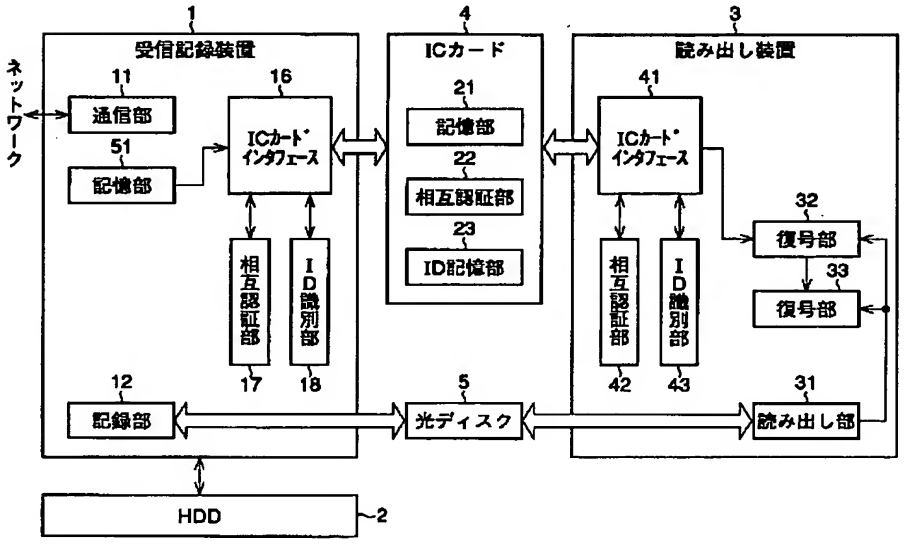
【図９】


移動用鍵記憶処理スタート
ICカードを装着する
S91
ICカードの再生装置IDを読み出す
S92
再生装置IDは、再生装置に登録されている？
S93
NO
YES
ICカードと相互認証する
S94
相互認証された？
S95
NO
YES
ICカードに移動用鍵を記憶させる
S96
エラー処理
S97
エンド

【図８】



【図１０】



フロントページの続き

(72)発明者　北村　出
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　北原　淳
東京都品川区北品川６丁目７番35号　ソニー株式会社内

Ｆターム(参考)　5D044 BC06 CC04 CC08 DE49 GK17 HH02 HL11
5K013 BA03 FA06 GA02 GA05